Verrou et clé : Listes d'accès dynamique

Contenu

Introduction Conditions préalables Conditions requises Components Used Conventions Considérations relatives à l'usurpation Performances Quand utiliser l'accès par clé et verrouillage Fonctionnement de l'accès par clé et verrouillage Exemple de configuration et de dépannage Diagramme du réseau Utilisation de TACACS+ Utilisation de RADIUS Informations connexes

Introduction

L'accès de verrou vous permet d'installer les listes d'accès dynamique qui accordent l'accès par utilisateur à une source/hôte de destination spécifique par un processus d'authentification de l'utilisateur. L'accès utilisateur est autorisé par le biais d'un pare-feu Cisco IOS[®] dynamiquement, sans aucun compromis dans les restrictions de sécurité.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Dans ce cas, l'environnement des travaux pratiques était constitué d'un routeur 2620 exécutant le logiciel Cisco IOS® Version 12.3(1). All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à <u>Conventions relatives aux conseils techniques Cisco.</u>

Considérations relatives à l'usurpation

L'accès par clé et verrouillage permet à un événement externe de placer une ouverture dans le pare-feu Cisco IOS Firewall. Après cette ouverture, le routeur est susceptible d'usurpation d'adresse source. Afin d'empêcher cela, fournir la prise en charge du chiffrement à l'aide du chiffrement IP avec authentification ou chiffrement.

L'usurpation d'adresse est un problème avec toutes les listes d'accès existantes. L'accès par verrouillage de clé ne résout pas ce problème.

Comme l'accès par clé et verrouillage introduit un chemin potentiel via votre pare-feu réseau, vous devez considérer l'accès dynamique. Un autre hôte, usurpant votre adresse authentifiée, obtient l'accès derrière le pare-feu. Avec l'accès dynamique, il est possible qu'un hôte non autorisé, usurpant votre adresse authentifiée, obtienne l'accès derrière le pare-feu. L'accès par verrouillage de clé ne cause pas de problème d'usurpation d'adresse. Le problème n'est identifié ici qu'en tant que préoccupation pour l'utilisateur.

Performances

Les performances sont affectées dans ces deux situations.

- Chaque liste d'accès dynamique force la reconstruction d'une liste d'accès sur le moteur de commutation de silicium (SSE). Cela entraîne un ralentissement momentané du chemin de commutation SSE.
- Les listes d'accès dynamiques nécessitent la fonction de délai d'inactivité (même si le délai d'attente est laissé à la valeur par défaut). Par conséquent, les listes d'accès dynamiques ne peuvent pas être commutées SSE. Ces entrées sont traitées dans le chemin de commutation rapide du protocole.

Observez les configurations des routeurs périphériques. Les utilisateurs distants créent des entrées de liste d'accès sur le routeur périphérique. La liste de contrôle d'accès se développe et se réduit dynamiquement. Les entrées sont supprimées dynamiquement de la liste après l'expiration du délai d'inactivité ou du délai maximal. Les grandes listes d'accès dégradent les performances de commutation de paquets.

Quand utiliser l'accès par clé et verrouillage

Voici deux exemples d'utilisation de l'accès par verrouillage et clé :

- Lorsque vous souhaitez qu'un hôte distant puisse accéder à un hôte de votre interréseau via Internet. L'accès par clé et verrouillage limite l'accès au-delà de votre pare-feu sur un hôte ou un réseau individuel.
- Lorsque vous souhaitez qu'un sous-ensemble d'hôtes d'un réseau accède à un hôte d'un réseau distant protégé par un pare-feu. Avec l'accès par clé et verrou, vous pouvez

uniquement activer un ensemble d'hôtes désiré pour obtenir l'accès en les faisant authentifier via un serveur TACACS+ ou RADIUS.

Fonctionnement de l'accès par clé et verrouillage

Ce processus décrit l'opération d'accès par clé et verrou.

- 1. Un utilisateur ouvre une session Telnet à un routeur périphérique configuré pour l'accès par verrouillage et clé.
- Le logiciel Cisco IOS reçoit le paquet Telnet. Il effectue un processus d'authentification des utilisateurs. L'utilisateur doit passer l'authentification avant d'autoriser l'accès. Le processus d'authentification est effectué par le routeur ou un serveur d'accès central tel qu'un serveur TACACS+ ou RADIUS.

Exemple de configuration et de dépannage



Diagramme du réseau

Cisco vous recommande d'utiliser un serveur TACACS+ pour votre processus de requête d'authentification. TACACS+ fournit des services d'authentification, d'autorisation et de comptabilité. Il fournit également la prise en charge des protocoles, la spécification des protocoles et une base de données de sécurité centralisée.

Vous pouvez authentifier l'utilisateur sur le routeur ou avec un serveur TACACS+ ou RADIUS.

Remarque : ces commandes sont globales sauf indication contraire.

Sur le routeur, vous avez besoin d'un nom d'utilisateur pour l'authentification locale de l'utilisateur.

username test password test

La présence de login local sur les lignes vty entraîne l'utilisation de ce nom d'utilisateur.

Si vous ne faites pas confiance à l'utilisateur pour émettre la commande **access-enable**, vous pouvez effectuer l'une des deux opérations suivantes :

Associez le délai d'attente à l'utilisateur par utilisateur.

```
username test autocommand access-enable host timeout 10
```

ou

• Forcer tous les utilisateurs de Telnet à avoir le même délai d'attente.

```
line vty 0 4
login local
autocommand access-enable host timeout 10
```

Remarque : Le **10** de la syntaxe correspond au délai d'*inactivité* de la liste d'accès. Il est remplacé par le délai d'attente absolu dans la liste d'accès dynamique.

Définissez une liste d'accès étendue qui est appliquée lorsqu'un utilisateur (n'importe quel utilisateur) se connecte au routeur et que la commande **access-enable** est exécutée. La durée maximale absolue de ce trou dans le filtre est de 15 minutes. Au bout de 15 minutes, le trou se ferme, que quelqu'un l'utilise ou non. La **liste de tests** de noms doit exister mais n'est pas significative. Limitez les réseaux auxquels l'utilisateur a accès en configurant l'adresse source ou de destination (ici, l'utilisateur n'est pas limité).

access-list 120 dynamic testlist timeout 15 permit ip any any

Définissez la liste de contrôle d'accès nécessaire pour bloquer tout le réseau, à l'exception de la possibilité d'établir une connexion Telnet avec le routeur (pour ouvrir un trou, l'utilisateur doit établir une connexion Telnet avec le routeur). L'adresse IP ici correspond à l'adresse IP Ethernet du routeur.

access-list 120 permit tcp any host 171.68.117.189 eq telnet

Il y a un refus implicite à la fin (non entré ici).

Appliquez cette liste d'accès à l'interface sur laquelle les utilisateurs entrent.

```
interface ethernet1
ip access-group 120 in
```

Tu as fini.

Voici à quoi ressemble le filtre sur le routeur en ce moment :

```
Router#show access-lists
Extended IP access list 120
```

10 Dynamic testlist permit ip any any log

20 permit tcp any host 171.68.117.189 eq telnet (68 matches)

Les utilisateurs qui accèdent à votre réseau interne ne peuvent rien voir tant qu'ils n'ont pas établi une connexion Telnet avec le routeur.

Remarque : Le **10** ici correspond au délai d'*inactivité* de la liste d'accès. Il est remplacé par le délai d'attente absolu dans la liste d'accès dynamique.

%telnet 2514A
Trying 171.68.117.189 ...
Connected to 2514A.network.com.
Escape character is '^]'.

User Access Verification

Username: **test** Password: **test**

Connection closed by foreign host. Le filtre ressemble à ceci.

Router#show access-lists
Extended IP access list 120
10 Dynamic testlist permit ip any any log
 permit ip host 171.68.109.158 any log (time left 394)
20 permit tcp any host 171.68.117.189 eq telnet (68 matches)

Il y a un trou dans le filtre pour cet utilisateur en fonction de l'adresse IP source. Quand quelqu'un d'autre fait ça, vous voyez *deux trous*.

Router#show ip access-lists 120
Extended IP access list 120
10 Dynamic testlist permit ip any any log
 permit ip host 171.68.109.64 any log
 permit ip host 171.68.109.158 any log
20 permit tcp any host 171.68.117.189 eq telnet (288 matches)

Ces utilisateurs peuvent avoir un accès IP complet à toute adresse IP de destination à partir de leur adresse IP *source*.

Utilisation de TACACS+

Configurer TACACS+

Configurez un serveur TACACS+ pour forcer l'authentification et l'autorisation sur le serveur TACACS+ afin d'utiliser TACACS+, comme le montre ce résultat :

aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+
tacacs-server host 10.48.66.53 key ciscol23

Complétez ces étapes pour configurer TACACS+ sur Cisco Secure ACS pour Windows :

- Ouvrez un navigateur Web. Entrez l'adresse de votre serveur ACS, sous la forme de http://<adresse_IP ou nom_DNS>:2002. (Cet exemple utilise un port par défaut de 2002.) Connectez-vous en tant qu'administrateur.
- 2. Cliquez sur **Configuration du réseau**. Cliquez sur **Ajouter une entrée** pour créer un groupe de périphériques réseau contenant les serveurs d'accès réseau (NAS). Entrez un nom pour le groupe et cliquez sur

CiccoSecure ACS - N	ferosoft Intrast Eiglants provided by Cisco Systems, Inc.	
fin fick your Pg	vantes jock gelp	
4-bad - + - 🥥	3 2 Brent Frontes State 3 3. 33. 3	
Address d http://fur2	SKJindev2.htm	<u>.</u> 50
Capen Sections	Network Configuration	
	Select	Help
Ber Stor	New Network Device Group	Network Device Group Name
Barelit offe Corporate	Network Dence My JWS	Network Device Group Name
Carlier dian	Subrit Cercel	To add a new Network Derice Group (NDG), type the name of the new group, and then click Submit Names can consist of our combination of combers
Configuration	2 Best to With	letters, or symbols. You can also assign users to an NDG at the group level.
949 Connel Dig Extensibler		Note: We recommend that you do not use spaces in NDG names.
Superity and Anticing		[Back to Top]
Soumettre		(Louintant

3. Cliquez sur **Ajouter une entrée** pour ajouter un client AAA (Authentication, Authorization and Accounting)

4-Back - + - 🥥	3 3 (Asech Manates Freds 3) 2-3 3 - 3	
Agdress All http://fur2	S85(Index2 htm	2
Cinco Seorean	Network Configuration	
	Select All Help	
User Setup Setup Setup Setup Setup Setup Setup Composition Seturity Configuration Seturity Configuration Seturity Configuration	My_NAS AAA Clients My_NAS AAA Clients AAA Client AAA Client IP Address None Defined Add Enty Search Adding a	evice Groups etwork Device Group Network Device Group Setwork Device Group or Network Devices & AA Client AA Client MAA Client FS AA Server AA Server
10 Extensi User	A My_NAS AAA Servers 2 Deleting a A	AAA Server ibution Table
BU Database	AAA Server AAA Server IP AAA Server Adding a Provide Address Type Sorting Prov	uxy Distribution Table Entry xy Distribution Table Entries
ucPet Online	None Defined - Editing a Pro	oxy Distribution Table Entry Proxy Distribution Table Entry
Documentation	Delete Group Bename Cancel	

4. Saisissez le nom d'hôte, l'adresse IP et la clé utilisée pour chiffrer la communication entre le serveur AAA et le serveur NAS. Sélectionnez TACACS+ (Cisco IOS) comme méthode d'authentification. Lorsque vous avez terminé, cliquez sur Soumettre +Redémarrer pour appliquer les modifications.



5. Cliquez sur **User Setup**, saisissez un ID utilisateur, puis cliquez sur **Add/Edit**.

Ele Edt yes fo	Microsoft Internet Explorer provided by Elsco Systems, Inc.	× Dix
- 6ad 0	3 3 Quest Marries 3reds 3 3. 33.	
Cisco Statema	User Setup	2 cho un -
Configuration	User: best Field Add/Edit List users beginning with letter/number: A B C D I K O B I 2 K L B H O F Q B S I U V H Z Y S Q A Z 2 S S I U V H Z Y S	User Setup and External User Databases Finding a Specific User in the CiscoSecure User Database Adding a User to the CiscoSecure User Database Listing Usernames that Begin with a Particular Character Listing All Usernames in the CiscoSecure User Database Changing a Username in the CiscoSecure User Database
Attribution Control Different Different Activity Differ Differ Differ Differ Differ	2 Back to Help	User Setup enables you to configure individual user information, add users, and delete users in the database. User Setup and External User Databases Before Cisco Secure ACS can authenticate users.

6. Sélectionnez une base de données pour authentifier l'utilisateur. (Dans cet exemple, l'utilisateur est « test » et la base de données interne de l'ACS est utilisée pour l'authentification). Entrez un mot de passe pour l'utilisateur et confirmez-



7. Choisissez le groupe auquel l'utilisateur est affecté et cochez la case **Utiliser le groupe**. Cliquez sur

Submit.				
🔄 transminister M	hrea <mark>t</mark> i ta esisten 👘 👘 👘	- 88		ک اماد 📭 👘
Die Die Sew USw	atan Ipala Usip			2 ²
48ad 🖷 - 🕲 🛛	김 🏠 🖏 Sand 🗊 Ferritz: 🥘 Noda 😗 🖏 🍎			
Agginess 😰 http:///27.0.	D.1 2489/			v (*So ⊔nis"
Cinco Secteur	User Setup			X
	supplying a separate CHAP password for a	-	11	
Di Dave	token and user slows CHAP authentication.			
Ligi Detug	enabled		 Access Disabled 	
			Deloting a Username	
	Group to which the user is assigned:		 Residentiative User Integeneties Research Authorities 	
Compression			 Group to which the ever is 	and and
Televant			- Callenda	
Condennes	Calibaria		 Client IP Address Autom 	
Configuration			 Advanced Suttings Natural: A success Restainti 	
In Links	n Tar group setting		 Max Services 	-
Cartiguette	O No calback alowed		 Usage Questos 	
Alexandresi Long	Calibark using this number		 Access Disable 	
			 Domologicality ACL: Advanced TACIA (D), Dec. 	• · · ·
Dia Detairen	O Dialeg ebent specifies caliback number		 TACACS+ Rashie Centre 	1
Ch. Reports and	O Use Windows Database calibrait, settings		IACACS+ Berlin Renow	
Address			 IACACS+ Outbound Page 	1.114
Desire Deservative	Client IP Address Assistment	ك.	 TACACS+ Shall Common 	d Antherleation
	subnit Cencel	<u> </u>	 <u>Commend</u> Authoritetion fr Mensurement Authoritien 	c Astronom Dancing
1				🗃 Internet 🦼

 8. Cliquez sur Configuration du groupe. Sélectionnez le groupe auquel l'utilisateur a été affecté à l'étape 7. Cliquez sur Modifier les paramètres.

CiscoSecure ACS - Microsoft Internet Explorer provided by Cisco Systems, Sir.		
Ele Edt yew Fgrontes Jools (pep		
Antes		
Agbress a http://flu:2585/index2.htm	🛫 🖓 Go Urês *	
Group Setup	×	
Select	Help 🖪	
User Scrop Group Stard Prutta Users in Group Edd Settings Parameterization	Default Group Group Users in Group Edit Settings Rename Group	
Interface Interface	Default Group If group mapping has not been configured, usernames that are not configured in the CiscoSecure Database are assigned to the Default Group by Cisco Secure ACS the first time they log in. The privileges and restrictions for the default group- are applied to first-time users. If you have upgraded from a previous version of Cisco Secure ACS and kept your database information, users will map as configured in the previous version.	

 Faites défiler jusqu'à la section TACACS+ Settings. Cochez la case pour Shell exec. Cochez la case de la commande Auto. Entrez la commande auto à exécuter après autorisation de l'utilisateur. (Cet exemple utilise la commande access-enable host timeout 10.) Cliquez sur Soumettre+Redémarrer.

CocoSecure ACS - Microsoft Internet Diplorer provided by Cisco Systems, Inc.				
Ele Edt you Fg	för fåt gen fyrates jods jeb			
4-Book - + - 🥥	3 3 Seath Gravates	Steda (J. J. J. J.		
Address Antop //flur2	585/index2.htm			<u>්</u> විණ Units ^ක
Cisco Systems	Group Setup			×
Laboration.	Jump To Acces	s Restrictions	Help	
Uper Setup	🗵 Shell (exec)			C
Legitore 1	C Access control list		Gro	up Settings to over IP (VoIP) Support
Setup	R Auto command	access-enable ho	Def	ault Time of Day Access Settings
Components	Calback ine		• <u>Cal</u>	back
The laters	E. Calback rotary		Max	work Access Restrictions
Configuration	E Idatina	and a second second second second second	Usa	ge Quotas
Zinter	1. sole table	L	• Ena	ble Options
Concise and	🗋 No callback verify	Enabled	• Tak	en Card Settings
Configuration	No escape	C Enabled	• Pass	record Aging Rules
Contraction of the second	No hangup	C Enabled	• <u>PA</u>	ssignment
Administration Control	Privilege level		Dow TAC	nioadabie ACLs 'ACS+ Settings
The Laternal User	T Treest		TAC	ACS+ Shell Command Authorization
90 Datauns	E Grandhau	to a second second	• Con	unand Authorization for Network Device
Reports and	L) Custom attributes		Ma	sagement Applications
An I working			• TAC	ACS+ Unknown Services
Dollare Documentation	1		- IET	F RADIUS Attributes
Submit Submit - Pestart Cancel • RADIUS Vendor-Specific Attributes				
				tocal intranet

Dépannage de TACACS+

Utilisez ces commandes debug sur le NAS pour résoudre les problèmes TACACS+.

Remarque : Consulter les <u>renseignements importants sur les commandes de débogage</u> avant d'utiliser les commandes de **débogage**.

- debug tacacs authentication Affiche des informations sur le processus d'authentification TACACS+. Uniquement disponible dans certaines versions de logiciel. Si non disponible, utilisez debug tacacs uniquement.
- debug tacacs autorisation Affiche des informations sur le processus d'autorisation TACACS+. Uniquement disponible dans certaines versions de logiciel. Si non disponible, utilisez debug tacacs uniquement.
- debug tacacs events : affiche les informations du processus d'assistance TACACS+.
 Uniquement disponible dans certaines versions de logiciel. Si non disponible, utilisez debug tacacs uniquement.

Utilisez ces commandes pour résoudre les problèmes AAA :

- debug aaa authentication Affiche des informations sur l'authentification AAA/TACACS+.
- debug aaa Authorization : affiche des informations sur l'autorisation AAA/TACACS+.

L'exemple de sortie **de débogage** ici montre un processus d'authentification et d'autorisation réussi sur le serveur ACS TACACS+.

```
Router#show debug
General OS:
 TACACS+ events debugging is on
 TACACS+ authentication debugging is on
 TACACS+ authorization debugging is on
 AAA Authentication debugging is on
 AAA Authorization debugging is on
_____
Router#
AAA/BIND(0000009): Bind i/f
AAA/AUTHEN/LOGIN (00000009): Pick method list 'default'
TPLUS: Queuing AAA Authentication request 9 for processing
TPLUS: processing authentication start request id 9
TPLUS: Authentication start packet created for 9()
TPLUS: Using server 10.48.66.53
TPLUS(0000009)/0/NB_WAIT/82A2E088: Started 5 sec timeout
TPLUS(0000009)/0/NB_WAIT: socket event 2
TPLUS(0000009)/0/NB_WAIT: wrote entire 36 bytes request
TPLUS(0000009)/0/READ: socket event 1
TPLUS(0000009)/0/READ: Would block while reading
TPLUS(0000009)/0/READ: socket event 1
TPLUS(0000009)/0/READ: read entire 12 header bytes
  (expect 16 bytes data)
TPLUS(0000009)/0/READ: socket event 1
TPLUS(0000009)/0/READ: read entire 28 bytes response
TPLUS(0000009)/0/82A2E088: Processing the reply packet
TPLUS: Received authen response status GET_USER (7)
TPLUS: Queuing AAA Authentication request 9 for processing
TPLUS: processing authentication continue request id 9
TPLUS: Authentication continue packet generated for 9
TPLUS(0000009)/0/WRITE/8347F3FC: Started 5 sec timeout
TPLUS(0000009)/0/WRITE: wrote entire 22 bytes request
TPLUS(0000009)/0/READ: socket event 1
TPLUS(0000009)/0/READ: read entire 12 header bytes
  (expect 16 bytes data)
TPLUS(0000009)/0/READ: socket event 1
TPLUS(0000009)/0/READ: read entire 28 bytes response
TPLUS(0000009)/0/8347F3FC: Processing the reply packet
```

TPLUS: Received authen response status GET_PASSWORD (8) TPLUS: Queuing AAA Authentication request 9 for processing TPLUS: processing authentication continue request id 9 TPLUS: Authentication continue packet generated for 9 TPLUS(0000009)/0/WRITE/8347EE4C: Started 5 sec timeout TPLUS(0000009)/0/WRITE: wrote entire 25 bytes request TPLUS(0000009)/0/READ: socket event 1 TPLUS(0000009)/0/READ: read entire 12 header bytes (expect 6 bytes data) TPLUS(0000009)/0/READ: socket event 1 TPLUS(0000009)/0/READ: read entire 18 bytes response TPLUS(0000009)/0/8347EE4C: Processing the reply packet TPLUS: Received authen response status PASS (2) AAA/AUTHOR (0x9): Pick method list 'default' TPLUS: Queuing AAA Authorization request 9 for processing TPLUS: processing authorization request id 9 TPLUS: Protocol set to NoneSkipping TPLUS: Sending AV service=shell TPLUS: Sending AV cmd TPLUS: Authorization request created for 9(tne-1) TPLUS: using previously set server 10.48.66.53 from group tacacs+ TPLUS(0000009)/0/NB_WAIT/8347F508: Started 5 sec timeout TPLUS(0000009)/0/NB_WAIT: socket event 2 TPLUS(0000009)/0/NB_WAIT: wrote entire 60 bytes request TPLUS(0000009)/0/READ: socket event 1 TPLUS(0000009)/0/READ: Would block while reading TPLUS(0000009)/0/READ: socket event 1 TPLUS(0000009)/0/READ: read entire 12 header bytes (expect 44 bytes data) TPLUS(0000009)/0/READ: socket event 1 TPLUS(0000009)/0/READ: read entire 56 bytes response TPLUS(0000009)/0/8347F508: Processing the reply packet TPLUS: Processed AV autocmd=access-enable host timeout 10 TPLUS: received authorization response for 9: PASS AAA/AUTHOR/EXEC(0000009): processing AV cmd= AAA/AUTHOR/EXEC(00000009): processing AV autocmd=access-enable host timeout 10 AAA/AUTHOR/EXEC(0000009): Authorization successful

Utilisation de RADIUS

Configurer RADIUS

Afin d'utiliser RADIUS, configurez un serveur RADIUS pour forcer l'authentification à être effectuée sur le serveur RADIUS avec les paramètres d'autorisation (la commande automatique) à être envoyée dans l'attribut 26 spécifique au fournisseur, comme indiqué ici :

aaa new-model
!
!
aaa authentication login default group radius local
aaa authorization exec default group radius local
radius-server host 10.48.66.53 auth-port 1645
 acct-port 1646 key cisco123

Complétez ces étapes pour configurer RADIUS sur Cisco Secure ACS pour Windows :

 Ouvrez un navigateur Web et entrez l'adresse de votre serveur ACS, sous la forme de http://<adresse_IP ou nom_DNS>:2002. (Cet exemple utilise un port par défaut de 2002.) Connectez-vous en tant qu'administrateur.

Ciscofecure ACS - Microsoft Internet Explorer provided by Cisco Systems, In

2. Cliquez sur **Configuration du réseau**. Cliquez sur **Ajouter une entrée** pour créer un groupe de périphériques réseau contenant le NAS. Entrez un nom pour le groupe et cliquez sur

fin fak yme fg	vantes jock 196	
4-lad - + - 🥥	2 2 2 See Press Bres 3 3. 3 2 - 3	
Agines Anto-/Per2	Sifjinde:2.htm	<u>।</u> २०
Cipen Stations	Network Configuration	
A.A.	Select	Hdp
Setup	New Network Device Group	<u>Network Device Group Name</u>
Server Servert Despensers Servert Catigorities Catigo	Network Derace Group Name Salarit Cancel 2 Sectores	Network Device Group Name To add a new Network Device Group (NDG), type the name of the new group, and then click Submit, Names can consist of any combination of numbers, letters, or symbols. You can also assign users to an NDG at the group level. Note: We recommend that you do not use spaces in NDG names. [Back to Top]
	1	l Institute

Soumettre.

3. Cliquez sur Ajouter une entrée pour ajouter un client AAA



(NAS).

4. Saisissez le nom d'hôte, l'adresse IP et la clé utilisée pour chiffrer la communication entre le serveur AAA et le serveur NAS. Sélectionnez **RADIUS (Cisco IOS/PIX)** comme méthode

d'authentification. Lorsque vous avez terminé, cliquez sur **Soumettre +Redémarrer** pour appliquer les

modifications.

Be Edt Yew Fa	Microsoft Internet Diploter provided by Cisco Systems, Inc. portesloolsloop	k qila T
4-Back	2 2 Seach Brannes Brads & 3. 3.	•
Address Antp://Ru:2	585(index2.htm	🛃 Pila Luks *
Cisco Svoramo	Network Configuration	×
Liter Seto	Add AAA Client	Holp AAA Client Hostname AAA Client IP Address
Sharedhotte	AAA Client Hostname	Key Network Device Group Authenticate Using
Setures Configuration	AAA Client IP 171.68.117.189	Single Connect TACACS+ AAA Client Log Update/Watchdog Packets from this AAA
Configuration	Key cisco123	Client Log RADIUS Tunneling Packets from this AAA
Configuration	Group	Replace RADIUS Port info with Username from this AAA Client
Di External User	Authenticate Using RADIUS (Criter) OS/PO	
Reports and Activity	Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	AAA Client Hostname
Discamentation	Chent	The AAA Client Hostname is the name assigned to the AAA client.
E) Done		Local retranst

5. Cliquez sur **User Setup**, saisissez un ID utilisateur, puis cliquez sur **Add/Edit**.

CiscoSecure ACS	Microsoft Internet Explorer provided by Lisco Systems, Inc.	
the tot year f	grantes jade 1940	
-Back 3)]] Quent Measure Breds ()].]] .	
Address Attp://flu	2585/index2.htm	
Ciaco Svarama	User Setup	×
	Select	Holp -
Components Components Components Components Configuration Con	User: Nest Field AddEdt List users beginning with letter/number: ABCREKOBIXES NOPOBITOVHIII QIZISESION	User Setup and External User Databases Finding a Specific User in the CiscoSecure User Database Adding a User to the CiscoSecure User Database Listing Usernames that Begin with a Particular <u>Character</u> Listing All Usernames in the CiscoSecure User <u>Database</u> Changing a Username in the CiscoSecure User <u>Database</u>
Advancestrution Control Ober Oxfordations Peperts and Activity Doctane Documentation	2 Buch for Sale	User Setup enables you to configure individual user information, add users, and delete users in the database. User Setup and External User Databases Before Cisco Secure ACS can asthenticate users

6. Sélectionnez une base de données pour authentifier l'utilisateur. (Dans cet exemple, l'utilisateur est « test » et la base de données interne de l'ACS est utilisée pour l'authentification). Entrez un mot de passe pour l'utilisateur et confirmez-



7. Choisissez le groupe auquel l'utilisateur est affecté et cochez la case **Utiliser le groupe**. Cliquez sur

Submit.				
📲 timmen i matter Mar	salis ta estidara 👘 👔 👘 👘	- 88		ک اعلے کا
Die Sait Vers Papart	a Danja Raje			25
4=Back + 🖷 - 🔘 👔	🕼 🕄 Sanci 🗇 Feverites 🎯 Noda 🔮 🖏 - 🍜			
Ağıras 📓 kepilliz7.0.0.	1.24 89 /			💌 🕫 େ ଆଧ୍ୟ "
Cinco Secrete	lser Setup			X
· · · ·	supplying a separate CHAP password for a		11	<u> </u>
	token und user allows CHAP automiration. This is sumerially parfit when belows parking is			
	conticd.		- Access Disablad	
			Deleting a December Eventeen Tree Tree	
C. Deviltante	Group to which the user is assigned:		- Person of Asthentication	
Conpressio	, , , , , , , , , , , , , , , , , , ,		· Group to which the near is as signed.	
Configuration			• Callerk	
Statutes	Caliback		Advanced Settings	
Configuration	* T		 Network Access Restrictions 	
Interfere	a Use group tenng		Max Service	
	Contraction of the second		<u>Usage Quetas</u> Assert Disable	
Control	Calbare using its burrys		Draninghing ACLs	
10 Starvillar	 Dishe cliest mariles athenis such as 		 Advanced TACACS+ Settings 	
3/12 Debaharra	O Ling tone specific cators for hereit		 TACACS+ Eachie Central 	
Kabita and	C OR WINCOWS DISIGNIS CHOSEN ISSUE		<u>IACACS+ Evolute Property</u> <u>TACACS+ Outburned Property</u>	
with I Dates	Client IP Address Assistant	-1	 TACACS+ Shall Command Asthering 	antima.
E horninia 4		<u> </u>	 Commond Authorization for Network 	Devise
	Submit Cencel		Management Applications	<u>ت</u> ادا
		_	[] [] [] [] [] [] [] [] [arret 🦽

 Cliquez sur Configuration du groupe et sélectionnez le groupe auquel l'utilisateur a été affecté à l'étape précédente. Cliquez sur Modifier les paramètres.

CiscoSecure ACS - Microsoft Internet Explorer provided by Lisco Systems, Iaz.			
Be Edit your Fyrontes Josh pelp			
4-Back	2 2 Seath Mercotes States 3 2 . 3 2 .		
Address http://fluc25	85/index2.htm	🛫 🖓 🐝 Uris 🐃	
Group Setup			
Contra Contrata	Select	Help	
Uter Setup Setup Composents Composents Configuration	Group : <mark>3 Group 3 (1 user) *</mark> Users in Group Edit Settings Plename Group	Default Group <u>Group Users in Group Edit Settings Rename Group </u>	
Configuration	2 Rack to Help	Default Group If group mapping has not been configured, usernames that are not configured in the CurcoSecure Database are assigned to the Default Group by Cinco Secure ACS the first time they	
Construction		log in. The privileges and restrictions for the default group- are applied to first-time users. If you have upgraded from a previous version of Cisco Secure ACS and kept your database information, users will map as configured in the previous version.	

 Faites défiler jusqu'à la section Cisco IOS/PIX RADIUS Attributes. Cochez la case correspondant à cisco-av-pair. Entrez la commande shell à exécuter après autorisation de l'utilisateur. (Cet exemple utilise shell : autocmd=access-enable host timeout 10.) Cliquez sur Soumettre+Redémarrer.



Dépannage de RADIUS

Utilisez ces commandes debug sur le NAS pour résoudre les problèmes RADIUS.

Remarque : Consulter les <u>renseignements importants sur les commandes de débogage</u> avant d'utiliser les commandes de **débogage**.

• debug radius : affiche les informations associées à RADIUS. Utilisez ces commandes pour résoudre les problèmes AAA :

• debug aaa authentication - Affiche des informations sur l'authentification AAA/TACACS+.

• debug aaa Authorization : affiche des informations sur l'autorisation AAA/TACACS+.

L'exemple de sortie **de débogage** ici montre un processus d'authentification et d'autorisation réussi sur l'ACS configuré pour RADIUS.

```
Router#show debug
General OS:
 AAA Authentication debugging is on
 AAA Authorization debugging is on
Radius protocol debugging is on
Radius packet protocol debugging is on
_____
Router#
AAA/BIND(0000003): Bind i/f
AAA/AUTHEN/LOGIN (0000003): Pick method list 'default'
RADIUS/ENCODE(0000003): ask "Username: "
RADIUS/ENCODE(0000003): send packet; GET_USER
RADIUS/ENCODE(0000003): ask "Password: "
RADIUS/ENCODE(0000003): send packet; GET_PASSWORD
RADIUS: AAA Unsupported [152] 5
RADIUS: 74 74 79
                                        [tty]
RADIUS(0000003): Storing nasport 66 in rad_db
RADIUS/ENCODE(0000003): dropping service type,
   "radius-server attribute 6 on-for-login-auth" is off
RADIUS(0000003): Config NAS IP: 0.0.0.0
RADIUS/ENCODE(0000003): acct_session_id: 1
RADIUS(0000003): sending
RADIUS/ENCODE: Best Local IP-Address 172.18.124.1
  for Radius-Server 10.48.66.53
RADIUS(0000003): Send Access-Request to 10.48.66.53:1645
  id 21645/1, len 77
RADIUS: authenticator 5A 95 1F EA A7 94 99 E5 -
  BE B5 07 BD E9 05 5B 5D
RADIUS:User-Name[1]7"test"RADIUS:User-Password[2]18*
RADIUS:NAS-Port[5]6RADIUS:NAS-Port-Type[61]6
                           [5] 6 66
                                      Virtual
                                                 [5]
RADIUS: Calling-Station-Id [31] 14 "171.68.109.158"
RADIUS: NAS-IP-Address [4] 6 171.68.117.189
RADIUS: Received from id 21645/1 10.48.66.53:1645,
  Access-Accept, len 93
RADIUS: authenticator 7C 14 7D CB 33 19 97 19 -
  68 4B C3 FC 25 21 47 CD
RADIUS:Vendor, Cisco[26]51RADIUS:Cisco AVpair[1]45
  "shell:autocmd=access-enable host timeout 10"
                  [25] 22
RADIUS: Class
RADIUS: 43 49 53 43 4F 41 43 53 3A 61 63 31 32 37 63 30
  [CISCOACS:ac127c0]
RADIUS: 31 2F 36 36
                                     [1/66]
RADIUS(0000003): Received from id 21645/1
AAA/AUTHOR/EXEC(0000003): processing AV
```

Informations connexes

- Sécurité par clé et verrouillage Cisco IOS
- Page de support TACACS/TACACS+
- TACACS+ dans la documentation d'IOS
- Page d'assistance RADIUS
- Demandes de commentaires (RFC)
- Support et documentation techniques Cisco Systems